

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-49443

(43) 公開日 平成10年(1998) 2月20日

(51) Int.Cl.⁵

G 0 6 F 12/14

識別記号

3 1 0

庁内整理番号

F I

G 0 6 F 12/14

技術表示箇所

3 1 0 K

審査請求 未請求 請求項の数 5 O L (全 9 頁)

(21) 出願番号

特願平8-205030

(22) 出願日

平成8年(1996) 8月2日

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 今田 美幸

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74) 代理人 弁理士 井出 直孝 (外1名)

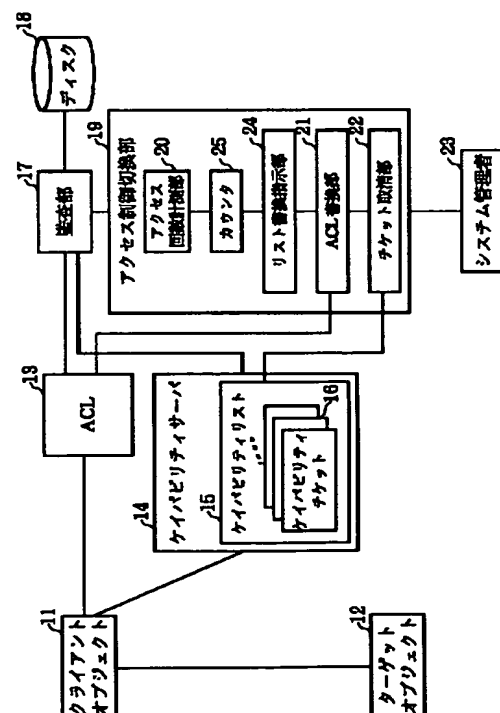
(54) 【発明の名称】 情報処理システム

(57) 【要約】

【課題】 クライアントオブジェクトからターゲットオブジェクトにアクセスする方法としてアクセス制御リストを用いる方法と、ケイパビリティリストを用いる方法がある。これらの使い分けは、システム管理者がシステムの立ち上がり時に設定するため、システム管理者がシステムの状態を把握したり、リストの書換えを行う必要がある。

【解決手段】 ケイパビリティリストのアクセス回数を計測し、頻繁にアクセスするターゲットオブジェクトに対するアクセス制御情報は、アクセス制御リストに転記する。

【効果】 システムの能力を有効に利用することができる。ユーザが頻繁にアクセスするターゲットオブジェクトのアクセスまでの時間を短縮できる。



【特許請求の範囲】

【請求項1】 アクセス制御リストにアクセス制御情報が記載されているターゲットオブジェクトに対してそのアクセス制御情報にしたがってアクセス可能であり、前記アクセス制御リストにアクセス制御情報の記載がなく、ケイパビリティリストにアクセス制御情報が記載されているターゲットオブジェクトに対しては前記ケイパビリティリストからケイパビリティチケットの発行を受けそのチケットによってそのケイパビリティリストに伴うアクセス制御情報にしたがってアクセス可能となるアクセス制御手段を備えた情報処理システムにおいて、前記ケイパビリティチケットの発行回数を計測記録する手段と、この計測記録する手段により記録されたケイパビリティチケット発行回数が所定数を越えたとき前記ケイパビリティリストに記載された当該アクセス制御情報を前記アクセス制御リストに自動的に転記する手段とを備えたことを特徴とする情報処理システム。

【請求項2】 前記アクセス制御リストに転記されたアクセス制御情報をその転記終了後に前記ケイパビリティリストから削除する手段を備えた請求項1記載の情報処理システム。

【請求項3】 アクセス制御リストにアクセス制御情報が記載されているターゲットオブジェクトに対してそのアクセス制御情報にしたがってアクセスされた回数をこのアクセス制御情報毎に計測記録する手段と、この計測記録する手段に記録された回数が小さいものから順に前記アクセス制御リストに記載された当該アクセス制御情報を自動的に削除する手段を備えた請求項1または2記載の情報処理システム。

【請求項4】 前記アクセス制御リストから削除されたアクセス制御情報を前記ケイパビリティリストに転記する手段を備えた請求項3記載の情報処理システム。

【請求項5】 アクセス制御リストにアクセス制御情報

【表1】

プログラム1のアクセス制御リスト：＜プロセス1， (Read, Execute)＞
 セグメントAのアクセス制御リスト：＜プロセス1， (Read, Write)＞
 セグメントBのアクセス制御リスト：＜プロセス2， Read ＞

となる。また、ケイパビリティリストに置き換えると、

【表2】

プロセス1のケイパビリティリスト：＜プログラム1， (Read, Execute)＞
 ＜セグメントA， (Read, Write) ＞
 プロセス2のケイパビリティリスト：＜セグメントB， Read ＞

となる。

【0004】 ケイパビリティ方式は、特定のプロセスの情報を局所化するのには有用であるため、分散システムでの適用には有効である。アクセス制御リストを分散リストで適用する場合には、プログラムやセグメントにおけるプロセス数が大きくなりがちであるため、アクセスが可能か否かを探索するために時間がかかる。

【0005】 一般には、ケイパビリティリストはクライ

が記載されているターゲットオブジェクトに対してそのアクセス制御情報にしたがってアクセスされた回数をこのアクセス制御情報毎に計測記録する第二の計測記録手段を備え、

この第二の計測記録手段には、きわめて大きな上限値が設定され、この計数結果がこの上限値を越えたときシステムの障害発生を通知する手段を備えた請求項3記載の情報処理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はソフトウェアの制御に利用する。本発明は情報処理システムの処理能力を有効に利用するための技術に関する。

【0002】

【従来の技術】 クライアントオブジェクトからターゲットオブジェクトに対するアクセス制御方法として、一般によく用いられているものとして、アクセス制御リスト（ACL）による方法と、ケイパビリティチケットによる方法とがある。アクセス制御リストは、アクセスできるターゲットオブジェクトの集合であるドメインとそれに対する操作の対（ドメイン、操作）からなるリストで、オブジェクト毎に規定される。ケイパビリティチケットは、アクセス制御リストの各行からなるオブジェクトとそのオブジェクトに対する操作の対（オブジェクト、操作）からなり、各ドメインに対して規定される。ケイパビリティチケットをリスト化したものをケイパビリティリストと呼ぶ。

【0003】 図9にオペレーティングシステムの制御単位であるプロセス毎にプログラムとセグメント毎の操作を示すファイルシステムのアクセス行列を示し、そのアクセス制御リストおよびケイパビリティリストの例を表1および表2に示す。図9に示したアクセス行列をアクセス制御リストに置き換えると、

クライアントオブジェクトが持つ方式が用いられている。このため、クライアントオブジェクトが勝手に偽造したり変形したりしないようにケイパビリティチケットの暗号化が必要となる。このため、クライアントオブジェクトはケイパビリティチケットの入手から実際にターゲットオブジェクトにアクセスするまでに要する時間はアクセス制御リストに比べてきわめて長い。

【0006】 一部のシステムには、アクセス制御リスト

3

とケイパビリティの両方を採用しているものがある。アクセス制御リストとケイパビリティリストを使いわけ

【0007】具体的には、まず、クライアントオブジェクトがアクセス制御リストにアクセスが許可されている
10 可否か問い合わせ、許可されている場合は、ターゲットオブジェクトに対しアクセスする。許可されていない場合には、ケイパビリティサーバなどにケイパビリティチケットの発行を要求し、ケイパビリティリストでアクセスが許可されているとき、ターゲットオブジェクトの秘密鍵などで暗号化されたケイパビリティチケットを保持した状態でアクセスを実行する。許可されていない場合は、ケイパビリティサーバなどが許可されていない旨をクライアントオブジェクトに通知する。

【0008】

【発明が解決しようとする課題】しかしながら、この方法は以下のような新たな問題を生じる。アクセス制御リストかケイパビリティリストのいずれでアクセス制御
20 を実行するかは、システム管理者かアプリケーション開発者がシステム立ち上げのときなどに設定する。このため、ユーザのシステムの使用形態が変わる毎に、システム管理者は上記リストを書き替えなければならない。これはすなわち、システム管理者がユーザやアプリケーションのシステム使用形態を常に把握しておく必要があることを意味する。システム管理者のこれらの変化の認識が遅れると、ケイパビリティチケットを頻繁に使用したアクセス制御を行うことになり、情報処理システムの処理性能が低下する。

【0009】本発明は、このような背景に行われたものであって、アクセス制御リストおよびケイパビリティリストの記載内容を自動的に最適な状態に書き換えることができる情報処理システムを提供することを目的とする。本発明は、システム管理者がシステム使用形態を常時監視する必要のない情報処理システムを提供することを目的とする。本発明は、システムの能力を有効に利用することができる情報処理システムを提供することを目的とする。本発明は、システムの障害を自動的に検出することができる情報処理システムを提供することを目的とする。本発明は、ユーザが速やかに希望するターゲットオブジェクトにアクセスすることができる情報処理システムを提供することを目的とする。

【0010】

【課題を解決するための手段】本発明は、実行中の処理とは非同期に、システム管理者を介することなく、ケイパビリティリストからアクセス制御リストにアクセス制御
40 を移し換えることを特徴とする。

【0011】すなわち、本発明は情報処理システムであって、アクセス制御リストにアクセス制御情報が記載されているターゲットオブジェクトに対してそのアクセス
50

4

制御情報にしたがってアクセス可能であり、前記アクセス制御リストにアクセス制御情報の記載がなくケイパビリティリストにアクセス制御情報が記載されているターゲットオブジェクトに対しては前記ケイパビリティリストからケイパビリティチケットの発行を受けそのチケットによってそのケイパビリティリストに伴うアクセス制御情報にしたがってアクセス可能となるアクセス制御手段を備えた情報処理システムである。本発明の特徴とするところは、前記ケイパビリティチケットの発行回数を計測記録する手段と、この計測記録する手段により記録されたケイパビリティチケット発行回数が所定数を越えたとき前記ケイパビリティリストに記載された当該アクセス制御情報を前記アクセス制御リストに自動的に転記する手段とを備えたところにある。

【0012】これにより、ケイパビリティリストに記載されているアクセス制御情報の内で、アクセスが頻繁に行われるターゲットオブジェクトのアクセス制御情報については、アクセス制御リストに自動的に転記されるため、アクセスまでに要する時間をアクセスが頻繁に行われるターゲットオブジェクトについて短縮することができる。

【0013】前記アクセス制御リストに転記されたアクセス制御情報をその転記終了後に前記ケイパビリティリストから削除する手段を備えることが望ましい。

【0014】また、アクセス制御リストにアクセス制御情報が記載されているターゲットオブジェクトに対してそのアクセス制御情報にしたがってアクセスされた回数をこのアクセス制御情報毎に計測記録する手段と、この計測記録する手段に記録された回数が小さいものから順に前記アクセス制御リストに記載された当該アクセス制御情報を自動的に削除する手段を備える構成とすることもできる。

【0015】これにより、アクセス制御リストにアクセス制御情報が記載されているターゲットオブジェクトの中で、アクセス頻度が低く、アクセス制御情報をアクセス制御リストに記載する意味を持たないターゲットオブジェクトが存在するときには、そのアクセス制御情報を削除することにより、アクセス制御リストの書き込み容量を低減させないように保つことができる。

【0016】このとき、前記アクセス制御リストから削除されたアクセス制御情報を前記ケイパビリティリストに転記する手段を備える構成としてもよい。

【0017】アクセス制御リストにアクセス制御情報が記載されているターゲットオブジェクトに対してそのアクセス制御情報にしたがってアクセスされた回数をこのアクセス制御情報毎に計測記録する第二の計測記録手段を備え、この第二の計測記録手段には、きわめて大きな上限値が設定され、この計数結果がこの上限値を越えたときシステムの障害発生を通知する手段を備える構成としてもよい。これにより、無限ループなどのようなシス

テム障害を検出することができる。

【0018】

【発明の実施の形態】

【0019】

【実施例】

（第一実施例）本発明第一実施例の構成を図1を参照して説明する。図1は本発明第一実施例の全体構成図である。

【0020】本発明は情報処理システムであって、アクセス制御リスト13にアクセス制御情報が記載されているターゲットオブジェクト12に対してそのアクセス制御情報にしたがってアクセス可能であり、アクセス制御リスト13にアクセス制御情報の記載がなくケイパビリティリスト15にアクセス制御情報が記載されているターゲットオブジェクト12に対してはケイパビリティリスト15からケイパビリティチケット16の発行を受けそのチケットによってそのケイパビリティリスト15に伴うアクセス制御情報にしたがってアクセス可能となるアクセス制御手段としてのアクセス制御切換部19を備えた情報処理システムである。

【0021】ここで、本発明の特徴とするところは、ケイパビリティチケット16の発行回数を計測記録する手段としてのアクセス回数計測部20およびカウンタ25と、このアクセス回数計測部20およびカウンタ25により記録されたケイパビリティチケット発行回数が所定数を越えたときケイパビリティリスト15に記載された当該アクセス制御情報をアクセス制御リスト13に自動的に転記する手段としてのリスト書換指示部24およびアクセス制御リスト（ACLと略す）書換部21とを備えたところにある。

【0022】アクセス制御リスト13に転記されたアクセス制御情報をその転記終了後にケイパビリティリスト15から削除する手段としてのチケット取消部22を備えている。

【0023】本発明第一実施例の動作を説明する。本発明第一実施例として、セキュリティ機能として欠かすことのできない監査部17と組み合わせた場合を示す。図1において、11はクライアントオブジェクトであり、12はターゲットオブジェクトであり、13はアクセス制御リストであり、15はケイパビリティリストであり、16はケイパビリティチケットであり、14はクライアントオブジェクトに対するケイパビリティチケットの発行要求受け付けおよび発行を行うケイパビリティサーバであり、17は監査部であり、18はディスクであり、19はアクセス制御切換部であり、20はアクセス回数計測部であり、21はアクセス制御リスト書換部であり、22はチケット取消部であり、23はシステム管理者であり、24はリスト書換指示部である。

【0024】図2は本発明第一実施例の通常処理におけるアクセス制御の手順を示すフローチャートであるが、

まず、通常処理におけるアクセス制御手順の説明を図2を参照して行う。クライアントオブジェクト11からターゲットオブジェクト12への呼び出しを行うとき（101）、クライアントオブジェクト11はアクセス制御リスト（ACLと略す）13でターゲットオブジェクト12にアクセス可能か否か確認する（102）。アクセス可能であれば、ターゲットオブジェクトへのアクセスを開始する（103、104）。アクセスが不可能な場合には、クライアントオブジェクト11は自己のIDとパスワードをケイパビリティサーバ14に提示し、ケイパビリティチケット16の発行を要求する（103、105）。ケイパビリティサーバ14はケイパビリティリスト15を検索して、アクセスが可能か否か確認する（106）。アクセスが可能なとき、ケイパビリティサーバ14はクライアントオブジェクト11に対してターゲットオブジェクトが提示した鍵を使って暗号化したケイパビリティチケット16をクライアントオブジェクト11に返送する（108）。クライアントオブジェクト11はターゲットオブジェクトの提示した鍵で暗号化したケイパビリティチケット16をターゲットオブジェクト12に提示して、アクセス許可をターゲットオブジェクト12から返送されると同時にアクセスを開始する（109）。アクセスが不可能な場合には、クライアントオブジェクト11に対し、ターゲットオブジェクト12へのアクセスが不可能であることを通知する（110）。

【0025】このフローチャートは、通常処理とは非同期に監査部17を用いて主メモリなどに書込み（104、108、110）、一定の周期でディスク18に書込む。

【0026】図3は本発明第一実施例のアクセス制御切換え手順を示すフローチャートである。図4はプログラム1のアクセス制御リストおよびプロセス2のケイパビリティリストにおけるアクセスの許可回数の例を示す図である。次に、本発明におけるアクセス制御の手順の説明を図3を用いて行う。監査部17で記録しているアクセス情報をアクセス制御切換部19が定期的にルックインし、クライアントオブジェクト11がターゲットオブジェクト12に対して呼び出しを行うために、アクセス制御リスト13やケイパビリティリスト15を参照し、アクセスの可能性を確認する（202）。アクセスが許可されていた場合には、アクセス回数計測部20で、図4に示すような情報をクライアントオブジェクトID

（1）、ターゲットオブジェクトID（2）、アクセス回数（3）をアクセス制御リスト13とケイパビリティリスト15毎に採取する（203、204）。例えば、図4では、クライアントオブジェクトID（1）のプログラム1がターゲットオブジェクトID（2）のプロセス1にアクセス制御リスト13を使用してアクセスした回数が3回であるという具合にである。アクセスが許可

7

されていない場合には、図4に示すデータの更新は行わない(203、210)。

【0027】図3において、クライアントオブジェクト11とターゲットオブジェクト12の対のアクセス回数がカウンタ25にあらかじめ設定してある回数より多くなった(オーバーフローした)場合には(205)、アクセス制御リスト書換指示部24を介し(211)、図4を参照して、カウンタ25がオーバーフローしたケイパビリティチケット16のオブジェクトと操作の対を図9および表1、表2を用いて説明したような形式でドメインと操作の対に変換し、アクセス制御リスト書換部21によりアクセス制御リスト13に追加する(208)。カウンタ25がオーバーフローしたケイパビリティチケット16は、チケット取消部22でケイパビリティリスト15から削除する。このとき、アクセス回数計測部20上にある図4のデータも書換える。

【0028】図3において、クライアントオブジェクト11とターゲットオブジェクト12の対のアクセス回数があらかじめ設定してある回数より多くなっていないとき(205)、上記のような処理は実行しない(210)。アクセス制御リスト13やケイパビリティリスト15からの追加や削除は(206~208)、必要ならばシステム管理者23に報告する(209)。

【0029】上記により、高信頼化のために設置した監
[表3]

アクセス制御リスト13の内部構造: <ドメイン名, 操作, アクセス回数>
プログラム1のアクセス制御リスト: <プロセス1, (Read, Execute), 1>
セグメントAのアクセス制御リスト: <プロセス2, (Read, Write), 0>
セグメントBのアクセス制御リスト: <プロセス2, Read, 8>

[表4]

ケイパビリティリストの内部構造: <オブジェクト名, 操作, アクセス回数>
プロセス1のケイパビリティリスト: <プロセス1, (Read, Execute), 1>
<セグメントA, (Read, Write), 3>
プロセス2のケイパビリティリスト: <セグメントB, Read, 0>

のようになる。

【0032】通常処理におけるアクセス制御の手順の説明を図6を用いて行う。クライアントオブジェクト11からターゲットオブジェクト12への呼び出しを行うとき(101)、クライアントオブジェクト11はアクセス制御リスト13でターゲットオブジェクト12にアクセス可能か否か確認する(102)。

【0033】アクセスが可能なとき(103)、表3の当該ドメインと操作の対のアクセス回数計測部20₁の値を更新する(1001)。そして、ターゲットオブジェクト12へのアクセスを開始する(104)。

【0034】アクセス制御リスト13でのアクセスが許可されないとき、クライアントオブジェクト11は自己のIDとパスワードをケイパビリティサーバ14に提示し、ケイパビリティチケット16の発行を要求する(103、105)。ケイパビリティサーバ14はケイパビ

8

査部17に記録したデータをもとに、システム管理者23の介在なしに、アクセス制御リスト13とケイパビリティリスト15の書換えが可能となる。

【0030】(第二実施例)本発明第二実施例を図5ないし図7を参照して説明する。図5は本発明第二実施例の全体構成である。図6は本発明第二実施例の通常処理におけるアクセス制御の手順を示すフローチャートである。図7は本発明第二実施例のアクセス制御切換え手順を示すフローチャートである。本発明第一実施例に示したアクセス回数計測部20のためのシステム資源が十分用意できない場合の対処策として、アクセス制御リスト13やケイパビリティリスト15にアクセス回数計測部20₁および20₂とカウンタ25を付加した場合の例を示す。

【0031】図5に示すように、本発明第一実施例で図1に示した構成から、監査部17、ディスク18、アクセス制御切換え部19を削除し、アクセス制御リスト書換部21にアクセス回数計測部20₁を、ケイパビリティリスト15にアクセス回数計測部20₂とカウンタ25を付加する。図9のようなアクセス行列を例にとると、アクセス制御リスト13とケイパビリティリスト14にアクセス回数計測部20₁および20₂を付加した場合の内部構成は、それぞれ、

リティリスト15を検索して、アクセスが可能か否か確認する(106)。

【0035】アクセスが可能なとき、表4の当該オブジェクトと操作の対のアクセス回数計測部20₂の値を更新する(1002)。ケイパビリティサーバ14はクライアントオブジェクト11に対してターゲットオブジェクトが提示した鍵を使って暗号化したケイパビリティチケット16をクライアントオブジェクト11に返送する(108)。クライアントオブジェクト11はターゲットオブジェクトの提示した鍵で暗号化したケイパビリティチケット16をターゲットオブジェクト12に提示して、アクセス許可をターゲットオブジェクト12から返送されると同時にアクセスを開始する(109)。

【0036】アクセスが不可能なとき、クライアントオブジェクト11に対し、ターゲットオブジェクト12へのアクセスが不可能であることを通知する(110)。

【0037】上記通常処理とは非同期に行われるアクセス制御切手順の説明を図7を用いて行う。クライアントオブジェクト11とターゲットオブジェクト12の対のアクセス回数がカウンタ25のオーバーフローにより、あらかじめ設定してある回数より多くなった場合(205)、リスト書換指示部24を介し(211)、アクセス回数の最も少ないクライアントオブジェクト11とターゲットオブジェクト12の対をアクセス制御リスト書換部21によりアクセス制御リストから削除し(206、207)、カウンタ25がオーバーフローした

クライアントオブジェクト16のオブジェクトと操作の対を図9および表1、表2で説明したような形式でドメインと操作の対に変換し、アクセス制御リスト書換部21によりアクセス制御リスト13に追加する(208)。

カウンタ25がオーバーフローしたクライアントオブジェクト16は、チケット取消部22でクライアントオブジェクト15から削除する。カウンタ25がオーバーフローしないとき(205)、上記のような処理は実行しない(210)。各リストからの追加や削除は(206~208)、必要ならばシステム管理者23に報告する(209)。

【0038】これにより、本発明第一実施例に比べて、アクセス回数計測のためのシステム資源をほとんど増やさずことなく、アクセス制御が可能となる。

【0039】(第三実施例)本発明第三実施例を図8を参照して説明する。図8は本発明第三実施例の全体構成図である。本発明第二実施例のアクセス制御リスト13に設置するアクセス回数計測部20₁に、無限ループのようなシステム障害を検出するためにアクセス回数計測手段としての障害検出カウンタ26をさらに設け、本発明がソフトウェア障害のようなシステム障害検出にも使用できる例について示す。

【0040】本発明第三実施例は、本発明第二実施例で図5に示したアクセス制御リスト13のアクセス回数計測部20₁に障害検出のための障害検出カウンタ26を追加したシステムである。

【0041】アクセス制御リスト13によりアクセス制御を行うターゲットオブジェクト12のアクセス回数が障害検出カウンタ26により著しく多いと判断したとき、すなわち、障害検出カウンタ26がオーバーフローしたとき、システムに障害が発生したとみなし、システム管理者23に通知する。

【0042】これにより、アクセス制御リスト13に対するアクセス頻度の計測をすることによって、無限ループなどのシステム障害を検出できる。

【0043】

【発明の効果】以上説明したように、本発明によれば、アクセス制御リストおよびクライアントオブジェクトの記載内容を自動的に最適な状態に書き換えることができる。したがって、システム管理者がシステム使用形態を常時監視する必要がない。これにより、システムの能力を有効に利用することができる。また、ユーザが希望するターゲットオブジェクトに速やかにアクセスすることができる。さらに、システムの障害を自動的に検出することができる。

【図面の簡単な説明】

【図1】本発明第一実施例の全体構成図。

【図2】本発明第一実施例の通常処理におけるアクセス制御の手順を示すフローチャート。

【図3】本発明第一実施例のアクセス制御切手順を示すフローチャート。

【図4】プログラム1のアクセス制御リストおよびプロセス2のクライアントオブジェクトにおけるアクセスの許可回数の例を示す図。

【図5】本発明第二実施例の全体構成。

【図6】本発明第二実施例の通常処理におけるアクセス制御の手順を示すフローチャート。

【図7】本発明第二実施例のアクセス制御切手順を示すフローチャート。

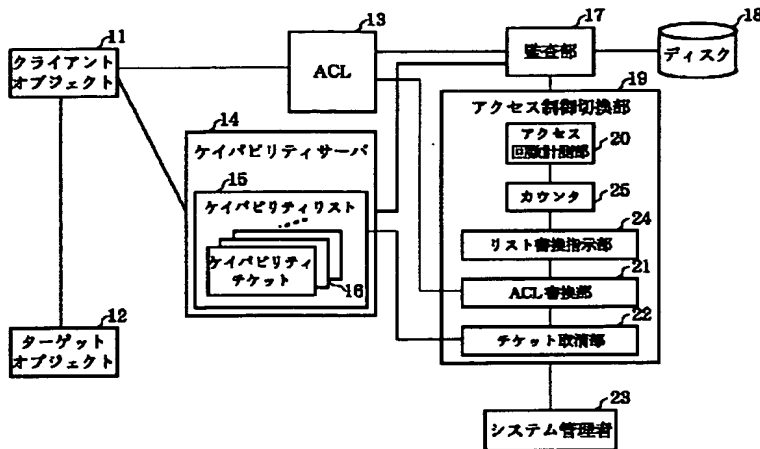
【図8】本発明第三実施例の全体構成図。

【図9】プロセス毎にプログラムとセグメント毎の操作を示すファイルシステムのアクセス行列を示す図。

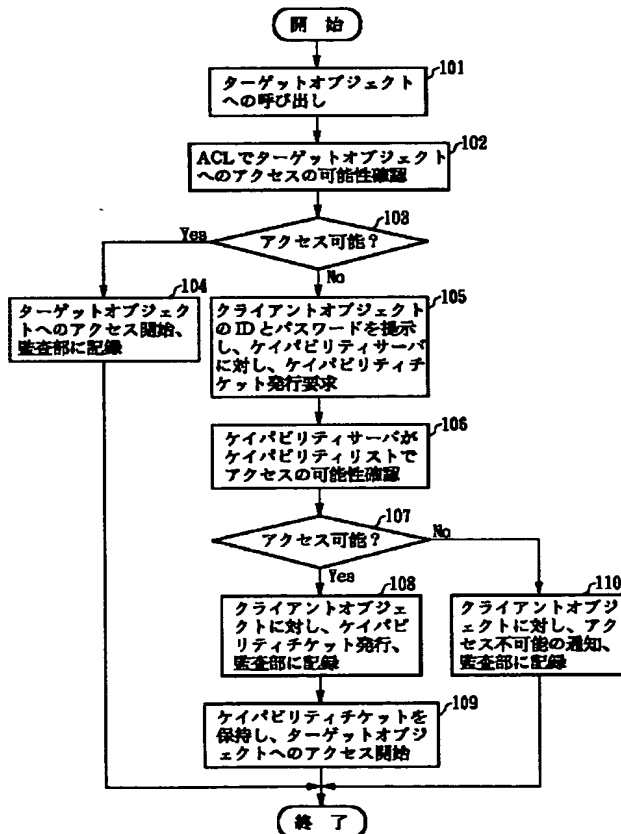
【符号の説明】

- 11 クライアントオブジェクト
- 12 ターゲットオブジェクト
- 13 アクセス制御リスト
- 14 クライアントオブジェクトサーバ
- 15 クライアントオブジェクトリスト
- 16 クライアントオブジェクトチケット
- 17 監査部
- 18 ディスク
- 19 アクセス制御切手部
- 20、20₁、20₂ アクセス回数計測部
- 21 アクセス制御リスト書換部
- 22 チケット取消部
- 23 システム管理者
- 24 リスト書換指示部
- 25 カウンタ
- 26 障害検出カウンタ

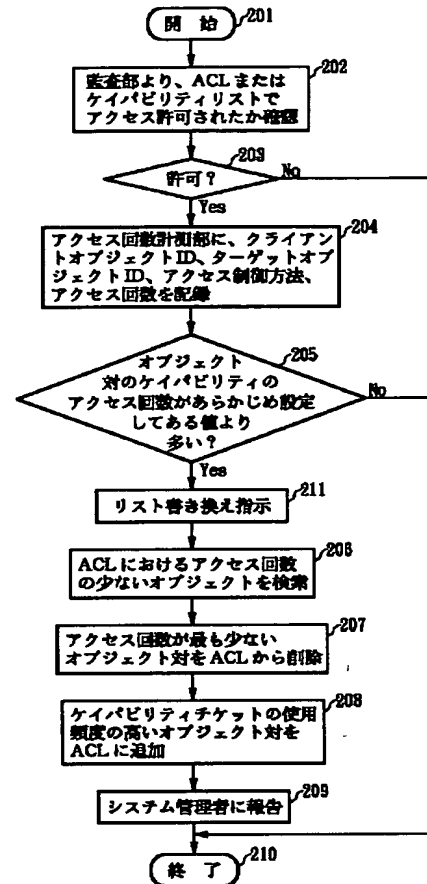
【図1】



【図2】



【図3】



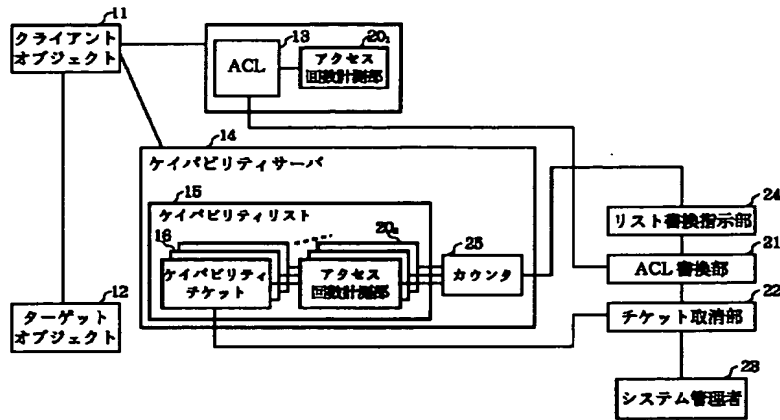
【図4】

クライアントオブジェクトID (1)	ターゲットオブジェクトID (2)	アクセス回数 (3)
プログラム1	プロセス1	2
セグメントB	プロセス2	1
.	.	.
.	.	.
.	.	.

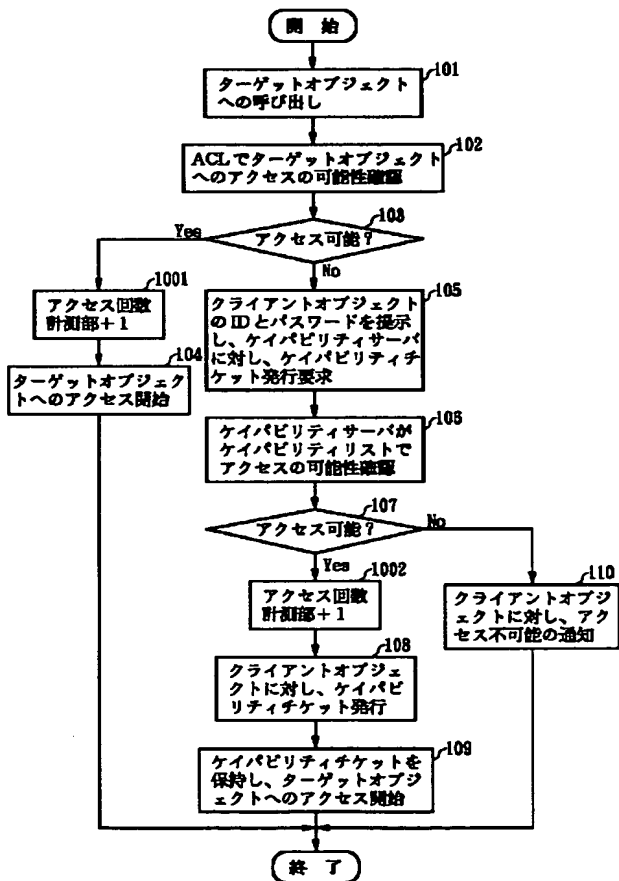
【図9】

オブジェクト プロセス	プログラム1	...	セグメントA	セグメントB
プロセス1	Read		Read	
プロセス2	Execute		Write	
.				Read
.				
.				

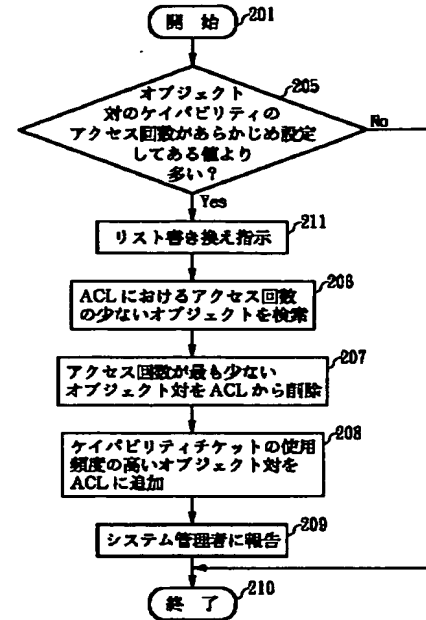
【図 5】



【図 6】



【図 7】



【図8】

